IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. Please cancel claim 40 without prejudice and amend claims 20 and 32 as follows:

Listing of Claims

1-19 (Cancelled).

20. (Currently Amended) A data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels, said data transmission controlling method comprising the steps of:

encapsulating the data to be transmitted in multiplexed fashion in accordance with a first protocol to form a section;

encrypting ~~at least one of data capsules~~ the section resulting from the encapsulation; [[and]]

supplementing the encrypted section with a section header and a section tailer;

~~encapsulating the encrypted data capsules by~~ dividing the encrypted [[data capsules]] supplemented section into a plurality of [[packets]] payloads in accordance with a second protocol [[,]]; and

adding transport stream headers to each payload to form packets;

wherein the first encapsulating step is done before the encrypting step and the first protocol pads a portion of 0 to 63 bits with a corresponding "1" as a suffix to the data, thereby maintaining a predetermined data length.

21. (Previously Presented) A data transmission controlling method according to claim 20, wherein said encapsulating in accordance with said first protocol supplements a real data part including said data to be transmitted to said data receiving means with an additional information part associated with said real data part.

22. (Original) A data transmission controlling method according to claim 21, wherein said additional information part includes destination address information identifying the data receiving means authorized to receive data included in said real data part.

23. (Original) A data transmission controlling method according to claim 22, wherein said destination address information is either individual or group destination address information.

24. (Original) A data transmission controlling method according to claim 22, wherein said data transmitting means possesses session keys corresponding to said destination address information, said session keys being used by said data transmitting means to encrypt information and data and by said receiving means to decrypt the encrypted information and data received; and

wherein said data transmitting means transmits in advance said session keys to the data receiving means authorized to receive the transmitted information and data in accordance with said destination address information.

25. (Original) A data transmission controlling method according to claim 24, wherein said session keys are updated at predetermined intervals.

26. (Original) A data transmission controlling method according to claim 24, wherein said session keys are transmitted over a communication channel permitting either unidirectional communication from said data transmitting means to said data receiving means or bidirectional communication therebetween.

27. (Previously Presented) A data transmission controlling method according to claim 21, wherein said encapsulating in accordance with said first protocol uniquely determines how said destination address information attached to said real data part is stored into said additional information part, said encrypting step further encrypting said real data part using a master key specific to the data receiving means corresponding to said destination address information.

28. (Original) A data transmission controlling method according to claim 22, wherein said additional information part provides a 48-bit space in which to accommodate said destination address information.

29. (Previously Presented) A data transmission controlling method according to claim 21, wherein the communication channel is in a broadcast data transmission system, including a satellite broadcast system, and said encapsulating in accordance with the first protocol encapsulates the data to be transmitted to said data receiving means in accordance with either the Internet protocol or the Ethernet protocol.

30. (Original) A data transmission controlling method according to claim 20, wherein said data receiving means is constituted as an IP router.

31. (Original) A data transmission controlling method according to claim 20, wherein said data receiving means is constituted as a bridge.

32. (Currently Amended) A data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels, said data transmission controlling method comprising the steps of:

encapsulating the data to be transmitted in multiplexed fashion in accordance with a first protocol to form a section, wherein the first protocol pads a portion of 0 to 63 bits with a corresponding "1" as a suffix to the data, thereby maintaining a predetermined data length;

encrypting the [[encapsulated data]] section using an encryption key;

supplementing the encrypted [[data]] section with encryption key information about said encryption key, a section header and a section tailer;

~~encapsulating the encrypted supplemented data by~~ dividing the encrypted supplemented [[data]] section into a plurality of [[packets]] payloads in accordance with a second protocol;

adding transport stream headers to each payload to form packets;

transmitting said [[plurality of]] packets from said data transmitting means to said data receiving means; and

decrypting said [[plurality of]] packets using one of a plurality of decryption keys which allow said data receiving means to decrypt said encrypted data and which are updatable, said one of

the decryption keys being selected in accordance with said encryption key information attached to said encrypted data.

33. (Previously Presented) A data transmission controlling method according to claim 32, wherein said plurality of decryption keys include a decryption key which is currently usable for decrypting said encrypted data received, and a decryption key which is to be used next to decrypt said encapsulated, encrypted data received; and

wherein said data decrypting step selects the currently usable decryption key based on said encryption key information.

34. (Original) A data transmission controlling method according to claim 33, wherein said encryption key and said decryption keys are session keys for encrypting information and data.

35. (Original) A data transmission controlling method according to claim 34, wherein said session keys are updated at predetermined intervals.

36. (Original) A data transmission controlling method according to claim 32, wherein said data receiving means is constituted as an IP router.

37. (Original) A data transmission controlling method according to claim 32, wherein said data receiving means is constituted as a bridge.

38. (Previously Presented) A data transmission controlling method according to claim 21, wherein said additional information part includes data to verify a communication channel.

39. (Previously Presented) A data transmission controlling method according to claim 32, wherein the supplemented data includes data to verify a communication channel.

40. (Cancelled).